

И. Ю. Могильных, Ф. И. Соловьева

# ОБ ОТДЕЛИМОСТИ КЛАССА ГОМОГЕННЫХ СОВЕРШЕННЫХ ДВОИЧНЫХ КОДОВ ОТ ТРАНЗИТИВНЫХ \*

## Аннотация

На примере класса совершенных двоичных кодов доказано существование двоичных гомогенных нетранзитивных кодов. Тем самым, с учетом ранее полученных результатов, установлена иерархическая картина меры линейности двоичных кодов, а именно имеет место строгое содержание класса двоичных линейных кодов в классе двоичных пропелинейных кодов, включающихся строго в класс двоичных транзитивных кодов, которые, в свою очередь, строго содержатся в классе двоичных гомогенных кодов. В работе выводится критерий транзитивности совершенных двоичных кодов ранга на единицу больше чем ранг кода Хэмминга той же длины.

## 1 Введение

Наиболее близкими по целому ряду свойств к линейным кодам (особенно по строению групп автоморфизмов) являются пропелинейные коды и транзитивные, все определения см. ниже. Вопрос о существовании транзитивных кодов, не являющихся пропелинейными, был впервые поставлен в 2006 г. Пухоле, Рифой, Ф.И.Соловьевой. Позднее, когда была получена классификация совершенных двоичных кодов длины 15 (см. [1]) и перечислены все транзитивные и гомогенные совершенные коды длины 15, естественно возник вопрос о существовании бесконечной серии двоичных гомогенных кодов, не являющихся транзитивными. На оба вопроса получены положительные ответы. На первый вопрос ответ получен в работе [2], где доказано, что известный двоичный код Беста длины 10 с кодовым расстоянием 4, будучи транзитивным, не является пропелинейным. Существование бесконечной серии транзитивных непропелинейных совершенных кодов доказано в работе [3]:

**Теорема 1.** *Для любого  $n \geq 15$  существуют совершенные двоичные транзитивные коды длины  $n$ , не являющиеся пропелинейными.*

Следует отметить, что в [3] было доказано, что только один из 201 неэквивалентного транзитивного совершенного кода длины 15 является непропелинейным. Ответ на вопрос о существовании двоичных гомогенных нетранзитивных кодов приводится в настоящей статье на примере совершенных кодов. Тем самым структура вложения классов упомянутых выше кодов, близких к линейным, имеет вид

$$L \subset Prl \subset Tr \subset Hom,$$

где  $L$  – класс линейных двоичных кодов,  $Prl$  – класс пропелинейных двоичных кодов,  $Tr$  – класс транзитивных двоичных кодов;  $Hom$  – класс гомогенных двоичных кодов.

---

\*Статья сдана в печать в журнал "Проблемы передачи информации". Работа выполнена при финансовой поддержке гранта Российский Научный Фонд 14-11-00555.

Приведем основные определения. Через  $F^n$  обозначим  $n$ -мерное метрическое пространство всех двоичных векторов длины  $n$  с метрикой Хэмминга. Произвольное подмножество векторов  $C$  из  $F^n$  называется двоичным кодом длины  $n$ . Код  $C$  называется *совершенным двоичным кодом* длины  $n$ , исправляющим одну ошибку, если для любого вектора  $x \in F^n$  найдется единственный вектор  $y$  из  $C$  на расстоянии один от  $x$ . Без ограничения общности будем рассматривать только *приведенные* коды, т.е. коды, содержащие нулевое слово  $0^n$  длины  $n$  (далее для краткости будем опускать термины двоичный и приведенный). Известно, что совершенные двоичные коды с расстоянием 3 существуют тогда и только тогда, когда  $n = 2^k - 1, k > 1$ . Широко известно, что для группы автоморфизмов  $\text{Aut}(F^n)$  пространства  $F^n$  справедливо

$$\text{Aut}(F^n) = F^n \rtimes S_n = \{(y, \pi) \mid y \in F^n, \pi \in S_n\},$$

где  $\rtimes$  – полупрямое произведение,  $S_n$  – симметрическая группа подстановок  $n$  координат векторов из  $F^n$ . *Группой автоморфизмов*  $\text{Aut}(C)$  произвольного кода  $C$  длины  $n$  называется стабилизатор кода  $C$  как множества по группе  $\text{Aut}(F^n)$ , т.е.

$$\text{Aut}(C) = \{(y, \pi) \mid y + \pi(C) = C\}.$$

*Группой симметрий* кода  $C$  называется множество  $\text{Sym}(C) = \{\pi \in S_n \mid \pi(C) = C\}$ . Очевидно, что  $\text{Sym}(C)$  – подгруппа группы  $\text{Aut}(C)$ .

Код  $C$  называется *транзитивным*, если его группа автоморфизмов содержит подгруппу, действующую транзитивно на всех его кодовых словах. Если эта подгруппа регулярна, т.е. ее порядок совпадает с мощностью кода, то такой код, следуя [4], называется *пропелинейным*. Для транзитивных кодов удобно пользоваться следующим, эквивалентным приведенному выше, определением: для каждого кодового слова  $y$  из  $C$  найдется подстановка  $\pi$  из  $S_n$  такая, что  $(y, \pi) \in \text{Aut}(C)$ , что означает  $y + \pi(C) = C$ , где  $\pi$  может не принадлежать группе симметрий  $\text{Sym}(C)$  кода  $C$ . Многие классы известных кодов являются транзитивными, см. обзор результатов, касающихся транзитивных кодов, в параграфе 4 работы [5].

*Система троек Штейнера*  $\text{STS}(n)$  порядка  $n$  определяется как система сочетаний из  $n$  элементов по три такая, что каждая неупорядоченная пара элементов содержится в точности в одной тройке. Известно, что совокупность носителей кодовых слов веса 3 в любом приведенном двоичном совершенном коде  $C$  длины  $n$  определяет систему троек Штейнера порядка  $n$ . Для кодового слова  $y$  кода  $C$  через  $\text{STS}(C, y)$  будем обозначать следующую систему троек Штейнера  $\{\text{supp}(x + y) : x \in C, d(x, y) = 3\}$ . Код  $C$  называется *гомогенным*, если для любого кодового слова  $y \in C$  система  $\text{STS}(C, y)$  *изоморфна*  $\text{STS}(C, 0^n)$ , то есть найдется подстановка  $\pi \in S_n$  такая, что  $\pi(\text{STS}(C, y)) = \text{STS}(C, 0^n)$ .

Нетрудно видеть, что всякий транзитивный код является гомогенным.

## 2 Строение группы вращений кодов Васильева

*Ядром*  $\text{Ker}(C)$  кода  $C$  называется совокупность его *периодов*, т.е. кодовых слов  $x \in C$  таких, что  $x + C = C$ . Рассмотрим *группу вращений*  $\text{Rot}(C)$  и *транслятор*  $\text{Tr}(C)$  кода  $C$ :

$$\text{Rot}(C) = \{\pi \in S_n \mid \exists y \in C : (\pi, y) \in \text{Aut}(C)\},$$

$$\text{Tr}(C) = \{y \in C \mid \exists \pi \in S_n : (\pi, y) \in \text{Aut}(C)\}.$$

Обозначим через  $\text{Rot}_y(C)$  класс смежности в  $\text{Rot}(C)$ , связанный с фиксированным кодовым словом  $y \in C$ :

$$\text{Rot}_y(C) = \{\pi \in S_n \mid (\pi, y) \in \text{Aut}(C)\}.$$

Ясно, что  $\text{Rot}_y(C) = \emptyset$  тогда и только тогда, когда  $y \notin \text{Tr}(C)$ . Имеет место следующее свойство, связывающее  $\text{Rot}(C)$  и  $\text{Tr}(C)$ :  $|\text{Aut}(C)| = |\text{Sym}(C)| \cdot |\text{Tr}(C)| = |\text{Rot}(C)| \cdot |\text{Ker}(C)|$ . Легко показать справедливость следующих утверждений.

**Утверждение 1.** *Для любого двоичного кода  $C$  выполняется*

$$\text{Sym}(C) \leq \text{Rot}(C) \leq \text{Sym}(\text{Ker}(C)).$$

В работе [6] исследована группа симметрий кодов Васильева. Для получения основного результата данной статьи нам потребуется изучить группу вращений кодов Васильева. Оказалось, что ряд результатов, справедливых для группы симметрий кодов Васильева, имеет место для группы вращений. Напомним необходимые определения из [6].

*Линейной  $i$ -компонентой* (далее кратко  *$i$ -компонентой*)  $R_i^n$  будем называть линейную оболочку троек кода  $C$  длины  $n$ , содержащих  $i$ ,  $i \in \{1, 2, \dots, n\}$ . Заметим, что в случае кода Хэмминга длины  $n$ ,  $R_i^n$  является его подкодом.

Пусть  $C$  – произвольный совершенный код длины  $n$ ,  $n = 2^k - 1$ ,  $\lambda : C \rightarrow \{0, 1\}$  – произвольная функция, удовлетворяющая  $\lambda(0^n) = 0$ . Рассмотрим коды  $C_\lambda = \{(y, \lambda(y), 0^n) \mid y \in C\}$  и  $R_{n+1}^{2n+1} = \{(x, |x|, x) \mid x \in F^n\}$ , где  $|x| = x_1 + \dots + x_n \pmod{2}$ . Оба кода имеют длину  $2n + 1$ , код  $R_{n+1}^{2n+1}$  является  $(n + 1)$ -компонентой. Пользуясь кодами  $C_\lambda$  и  $R_{n+1}^{2n+1}$ , определим двоичный совершенный код Васильева [7]:

$$V_C^\lambda = C_\lambda + R_{n+1}^{2n+1} = \{(x + y, |x| + \lambda(y), x) \mid x \in F^n, y \in C\} \quad (1)$$

длины  $2n + 1$ .

Заметим, что в силу того, что компонента  $R_{n+1}^{2n+1}$  является подпространством ядра кода Васильева, то для любого  $y \in V_C^\lambda$  и  $v \in R_{n+1}^{2n+1}$  верны следующие соотношения:

$$\text{STS}(V_C^\lambda, y) = \text{STS}(V_C^\lambda, y + v), \quad y \in \text{Tr}(C) \text{ тогда и только тогда, когда } y + v \in \text{Tr}(C).$$

Обозначим через  $t_i$  транспозицию, переводящую  $i$  в  $i + n + 1$ ,  $i \in I$ , где  $I = \{1, 2, \dots, n\}$ . Для вектора  $u \in F^n$  рассмотрим подстановку  $\tau_u = \prod_{i \in \text{supp}(u)} t_i$ . Обозначим совокупность всех подстановок, соответствующих  $F^n$ , через  $G$ , т.е.  $G = \{\tau_u \mid u \in F^n\}$ . Для произвольной подстановки

$$\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}$$

подстановка  $\sigma_\pi$ , называемая *дубликатом*, определяется следующим образом:

$$\sigma_\pi = \begin{pmatrix} 1 & 2 & \dots & n & n+1 & n+2 & n+3 & \dots & 2n+1 \\ \pi(1) & \pi(2) & \dots & \pi(n) & n+1 & \pi(1) + n + 1 & \pi(2) + n + 1 & \dots & \pi(n) + n + 1 \end{pmatrix}.$$

Множество всех дубликатов обозначается через  $D$ , т.е.  $D = \{\sigma_\pi \mid \pi \in S_n\}$ . Стабилизатор  $i$ -ой координаты группы вращений кода  $C$  обозначим через  $\text{St}_i(\text{Rot}(C))$ .

**Лемма 1.** *Для любого кода Васильева  $V_C^\lambda$  справедливо  $\text{St}_{n+1}(\text{Rot}(V_C^\lambda)) \leq D \times G$ .*

Доказательство этой леммы аналогично доказательству предложения 3 из [6], достаточно заменить  $\text{Sym}(V_C^\lambda)$  на  $\text{Rot}(V_C^\lambda)$  и использовать утверждение 1. Нам потребуется также следующая лемма (см. предложение 4 в работе [6]):

**Лемма 2.** *Для произвольных кода  $C$  длины  $n$  и определенной выше функции  $\lambda$  выполняется  $\tau_u((y, \lambda(y), 0^n)) = (y, \lambda(y), 0^n) + (y * u, 0, y * u)$  для любого  $y \in C$ , где  $y * u = (y_1 u_1, \dots, y_n u_n)$ .*

**Теорема 2.** Пусть  $V_C^\lambda$  – произвольный код Васильева,  $z = (y', \lambda(y'), 0^n) \in V_C^\lambda$ . Подстановка  $\rho_z$  принадлежит  $St_{n+1}(Rot_z(V_C^\lambda))$  тогда и только тогда, когда она может быть представлена композицией  $\rho_z = \sigma_{\pi_{y'}} \circ \tau_u$  для некоторых  $\pi_{y'} \in Rot_{y'}(C)$  и  $u \in F^n$  таких, что для любого  $y \in C$  выполняется соотношение

$$\lambda(y') + \lambda(y) + \lambda(y' + \pi_{y'}(y)) = u \cdot y, \quad (2)$$

где  $u \cdot y$  – скалярное произведение векторов  $u$  и  $y$  из  $F^n$ .

Заметим, что при  $y' = 0$  справедливо  $St_{n+1}(Rot_{y'}(V_C^\lambda)) = St_{n+1}(Sym(V_C^\lambda))$ , равенство (2) преобразуется в равенство  $\lambda(y) + \lambda(\pi(y)) = u \cdot y$  (см. определение  $\lambda$ -согласованности в [6]).

*Доказательство.* Рассмотрим произвольную подстановку  $\rho_z \in St_{n+1}(Rot_z(V_C^\lambda))$ , где  $z = (y', \lambda(y'), 0^n)$ . По лемме 1 имеем  $\rho_z = \sigma_{\pi_{y'}} \circ \tau_u$ , где  $u$  – некоторый вектор  $F^n$ , а  $\pi_{y'}$  некоторая подстановка из  $S_n$ . Покажем, что  $\pi_{y'} \in Rot_{y'}(C)$  и для всех  $y$  выполнено равенство (2).

Так как  $z + \rho_z(V_C^\lambda) = V_C^\lambda$ , то для любого  $y \in C$  имеем

$$(y', \lambda(y'), 0^n) + \sigma_{\pi_{y'}} \circ \tau_u(y, \lambda(y), 0^n) \in V_C^\lambda.$$

Согласно Лемме 2 и определению дубликатора, имеем  $\sigma_{\pi_{y'}} \circ \tau_u(y, \lambda(y), 0^n) = (\pi_{y'}(y + u * y), \lambda(y), \pi_{y'}(u * y))$ . Следовательно для всех  $y \in C$  вектор  $(y', \lambda(y'), 0^n) + \sigma_{\pi_{y'}} \circ \tau_u(y, \lambda(y), 0^n) = (y', \lambda(y'), 0^n) + (\pi_{y'}(y), \lambda(y) + u \cdot y, 0^n) + (\pi_{y'}(y * u), u \cdot y, \pi_{y'}(y * u)) = (y' + \pi_{y'}(y), \lambda(y') + \lambda(y) + u \cdot y, 0^n) + (\pi_{y'}(y * u), u \cdot y, \pi_{y'}(y * u))$  принадлежит  $V_C^\lambda$ . В силу того, что код Васильева  $V_C^\lambda$  представляет собой некоторую совокупность классов смежности по компоненте  $R_{n+1}^{2n+1}$ , то прибавление вектора  $(\pi_{y'}(y * u), u \cdot y, \pi_{y'}(y * u))$ , принадлежащего  $R_{n+1}^{2n+1}$ , к вектору  $(y' + \pi_{y'}(y), \lambda(y') + \lambda(y) + u \cdot y, 0^n)$  никак не влияет на свойство последнего принадлежать коду  $V_C^\lambda$  для любого  $y$  из кода  $C$ . Отсюда заключаем что  $\pi_{y'}$  принадлежит  $Rot_{y'}(C)$ , а равенство (2) выполняется для всех  $y$ .  $\square$

Заметим, что в работе [8] Д.С. Кротов и В.Н. Потапов предположили, что транзитивные коды ранга  $n - \log(n + 1) + 1$  следует искать в классе кодов Васильева с функцией, удовлетворяющей некоторому равенству, эквивалентному равенству (2), однако объяснения этому факту приведено не было. Также выполнение равенства (2) при  $\pi_{y'} = id$  для всех  $y, y'$  эквивалентно определению квадратичной функции, рассмотренной в той же работе.

**Следствие 1.** Пусть  $\lambda$  – нелинейная булева функция на коде Хэмминга  $H$ . Тогда  $y' \in Tr(V_H^\lambda)$  тогда и только тогда, когда найдутся  $\pi \in Sym(H)$ ,  $u \in F^n$  такие, что для всех  $y \in H$  выполнено  $\lambda(y') + \lambda(y) + \lambda(y' + \pi(y)) = u \cdot y$ .

*Доказательство.* Пусть  $\rho_z \in Rot_z(V_H^\lambda)$ . Заметим, что код, полученный из  $V_H^\lambda$  удалением  $j$ -й координаты будет линейным тогда и только тогда, когда  $j = (n + 1)/2$ . Следовательно, рассматривая равенство  $z + \rho_z(V_H^\lambda) = V_H^\lambda$ , приходим к выводу  $Rot_z(V_H^\lambda) = St_{n+1}(Rot_z(V_H^\lambda))$ , что в силу теоремы 2 дает требуемое.  $\square$

### 3 Гомогенные совершенные коды ранга $n - \log(n + 1) + 1$

В этом разделе докажем существование бесконечной серии гомогенных нетранзитивных совершенных кодов длины  $n$  для каждого допустимого  $n \geq 15$  ранга  $n - \log(n + 1) + 1$ . Построение этих кодов базируется на существовании гомогенных нетранзитивных совершенных кодов длины 15.

Для дальнейшего нам потребуется конструкция системы троек Штейнера Ассмуса и Маттсона [9] и ее связь с конструкцией Васильева, напомним их. Пусть  $S$  является STS( $n$ )

и  $\theta : S \rightarrow \{0, 1\}$  – произвольная булева функция на тройках  $S$ . Определим  $S^\theta$  – систему  $STS(2n+1)$  следующим образом:

- тройки  $\{i, n+1, i+n+1\}$  принадлежат  $S^\theta$  для любого  $i \in \{1, \dots, n\}$ ;
- если  $\theta(\{i, j, k\}) = 0$ , то тройки  $\{i, j, k\}, \{i, j+n+1, k+n+1\}, \{k, i+n+1, j+n+1\}, \{j, i+n+1, k+n+1\}$  принадлежат  $S^\theta$ ;
- если  $\theta(\{i, j, k\}) = 1$ , то тройки  $\{i+n+1, j+n+1, k+n+1\}, \{i, j, k+n+1\}, \{j, k, i+n+1\}, \{i, j, k+n+1\}$  принадлежат  $S^\theta$ .

**Утверждение 2.** Пусть  $C$  является совершенным кодом,  $\lambda : C \rightarrow \{0, 1\}$ ,  $z = (x+y, |x|, x)$  является кодовым словом кода  $V_C^\lambda$ . Тогда  $STS(V_C^\lambda, z)$  есть  $STS(C, y)^\theta$ , где  $\theta(\text{supp}(y+y')) = \lambda(y) + \lambda(y')$ , для  $y' \in C$ , таких что  $d(y', y) = 3$ .

### 3.1 Гомогенные нетранзитивные совершенные коды длины 15

Для  $n = 15$  были исследованы все совершенные коды ранга 12, оказалось, что среди них существует всего два гомогенных нетранзитивных совершенных кода – это коды, обозначаемые  $V22^1$  и  $V3^11$  согласно классификации С. А. Малюгина [10] двоичных совершенных кодов длины 15, полученных свитчингами из кода Хэмминга той же длины.

Произвольное кодовое слово  $x$  будем задавать его носителем  $\text{supp}(x) = \{i | x_i = 1\}$ . Пусть  $H$  – код Хэмминга длины 7, порожденный векторами  $\{1, 2, 3\}, \{1, 4, 5\}, \{1, 6, 7\}, \{2, 4, 6\}$ .

Код  $V22^1$  – код Васильева  $V_H^\lambda$ , см. (1), где  $\lambda(0^7) = \lambda(\{1, 6, 7\}) = \lambda(\{1, 3, 5, 7\}) = \lambda(1^7) = 0$ , на остальных кодовых словах кода  $H$  значение функции  $\lambda$  равно 1.

Код  $V3^11$  – это код Васильева  $V_H^\lambda$ , где  $\lambda(0^7) = \lambda(\{1, 6, 7\}) = \lambda(\{2, 4, 6\}) = \lambda(\{4, 5, 6, 7\}) = 0$ , на прочих кодовых словах кода  $H$  значение  $\lambda$  равно 1.

**Лемма 3.** Коды  $V3^11$  и  $V22^1$  являются гомогенными.

*Доказательство.* Заметим, что определенные выше функции  $\lambda$  на коде  $H^7$  обладают следующим свойством: для любого кодового слова  $y \in H^7$  выполняется  $|\{y' \in H^7 : d(y', y) = 3, \lambda(y) = \lambda(y')\}|$  принимает следующие значения: 1, 2, 5, 6. Принимая во внимание утверждение 2 покажем, что  $S^\theta$  изоморфна  $S^{\theta'}$ , где  $\theta$  и  $\theta'$  – произвольные булевы функции на системе троек Штейнера  $S$  порядка 7 с 1, 2, 5 или 6 нулями.

Вначале докажем утверждение для функций с одним нулем или двумя нулями. Если  $\theta$  и  $\theta'$  имеют одинаковое число нулей, то в силу 2-транзитивности группы симметрий системы троек Штейнера порядка 7 (как двоичного кода) найдется подстановка  $\pi$ , переводящая нули  $\theta$  в нули  $\theta'$ . Тогда подстановка  $\sigma_\pi$  переводит тройки  $S^\theta$  в тройки  $S^{\theta'}$ .

Пусть  $\theta$  имеет один ноль, а  $\theta'$  имеет два нуля. В силу сказанного выше, без ограничения общности все тройки, на которых функции  $\theta$  и  $\theta'$  принимают значение ноль, являются тройками системы  $S$ , которые имеют один общий элемент, скажем  $i$ .

Заметим, что тройки  $\{i, j, k\}, \{i, j+8, k+8\}, \{k, i+8, j+8\}, \{j, i+8, k+8\}$  переходят в тройки  $\{i+8, j+8, k+8\}, \{i, j, k+8\}, \{j, k, i+8\}, \{i, j, k+8\}$  с помощью транспозиции  $t_i = (i, i+8)$ . Так как эти совокупности троек есть в точности совокупности, индуцируемые тройкой  $\{i, j, k\}$  в конструкции Ассмуса и Маттсона при  $\theta(\{i, j, k\}) = 0$  или 1, то подстановка  $(i, i+8)$  переводит все тройки  $S^\theta$ , содержащие  $i$ , в тройки  $S^{\theta'}$ , содержащие  $i+8$ . Следовательно,  $t_i(S^\theta) = S^{\theta'}$ .

Случай когда  $S^\theta$  является системой троек, где  $\theta$  принимает 5 или 6 нулей, сводится к рассмотренному выше случаю с одним или двумя нулями для функции  $\theta$  с помощью подстановки  $\tau_{17}$ , которая меняет местами координаты  $i$  и  $i+8$  для любого  $i \in \{1, \dots, 7\}$ . При этом система троек  $\tau_{17}(S^\theta)$  получается из  $S$  применением функции с одним нулем или двумя нулями.  $\square$

**Лемма 4.** Коды  $V3^{11}$  и  $V22^1$  не являются транзитивными.

*Доказательство.* Напомним, что  $Rot(H) = Sym(H)$ . Докажем, что для кода  $V3^{11}$  нарушается равенство (2), где  $\pi$  пробегает  $Sym(H)$ , а  $y' = 1^7$ . Поскольку  $\lambda(1^7) = 1$ , условие (2) преобразуется в следующее

$$\lambda(1^7 + \pi(y)) = u \cdot y + \lambda(y) + 1. \quad (3)$$

Рассмотрим правую часть (3). Заметим, что равенство  $u \cdot y = 0$  задает гиперпространство  $U = \{y : y \cdot u = 0\}$  в коде Хэмминга  $H$  длины 7, число таких гиперпространств равно числу ненулевых точек в  $H$ , т.е. равно 15. Справедливы следующие случаи:

- а) вектор  $u$  принадлежит коду  $H^\perp$  – ортогональному к коду  $H$ ;
- б) имеем 7 подпространств –  $i$ -компонент кода  $H$ ,  $i \in \{1, 2, \dots, 7\}$ , имеющих весовое распределение, состоящее из нулевого вектора, трех кодовых слов веса 3, трех кодовых слов веса 4 и единичного кодового слова кода  $H$ , например  $R_1^7 = \langle \{1, 2, 3\}, \{1, 4, 5\}, \{1, 6, 7\} \rangle$ ;
- с) имеем 7 подпространств, содержащих нулевой вектор, четыре кодовых слова веса 3 и три кодовых слова веса 4 кода  $H$ , например  $\langle \{1, 6, 7\}, \{2, 4, 6\}, \{4, 5, 6, 7\} \rangle$ .

В случае а) в силу  $u \cdot y = 0$  соотношение (3) примет вид  $\lambda(1^7 + \pi(y)) = \lambda(y) + 1$ , из которого следует, что функция  $\lambda$  имеет одинаковое число 0 и 1, что противоречит ее определению.

В случае б) снова исследуем соотношение (3). Без ограничения общности полагаем, что  $R_1^7 \subset U$ . Рассмотрим обе части равенства (3) при  $y$ , пробегающих множество кодовых слов веса 3 в коде  $H$ . С одной стороны,  $1^7 + \pi(y')$  пробегает множество векторов веса 4, следовательно  $\lambda(1^7 + \pi(y'))$  равно 0 только в одном случае и 1 в шести. С другой стороны,  $\lambda(y) + 1$  будет равно 0 на пяти кодовых словах, 1 – на двух кодовых словах,  $u \cdot y = 0$  для трех кодовых слов  $\{1, 2, 3\}, \{1, 4, 5\}, \{1, 6, 7\}$ . Следовательно, для кодовых слов  $y$  таких, что  $\lambda(y) = 0$ , должно необходимо выполняться  $u \cdot y = 0$ . Аналогичное утверждение получим в случае, когда  $y$  пробегает множество кодовых слов веса 4 в коде  $H$ :  $\lambda(1^7 + \pi(y))$  принимает значение 0 на двух кодовых словах и 1 на пяти. Другими словами, все нули функции  $\lambda(y)$ , заданные на коде  $H$ , должны принадлежать  $U$ , т.е. случай б) невозможен.

Для каждого из 7 подпространств в случае с) снова рассмотрим вектор  $y$ , пробегающий множество кодовых слов веса 3 в коде  $H$  и убеждаемся, что  $u \cdot y + \lambda(y) + 1$  будет равно 0 как минимум на двух кодовых словах, в то время как левая часть  $\lambda(1^7 + \pi(y))$  принимает значение 0 только на одном кодовом слове и 1 – на шести кодовых словах, противоречие.

Нетранзитивность кода  $V22^1$  доказывается аналогично.  $\square$

## 4 Бесконечная серия гомогенных нетранзитивных кодов

Покажем, что с помощью конструкции Васильева из гомогенных совершенных кодов можно получать гомогенные коды большей длины.

**Теорема 3.** Если  $C$  – произвольный гомогенный совершенный код, то код Васильева  $V_C^\lambda$  при  $\lambda \equiv 0$  является гомогенным.

*Доказательство.* Обозначим код Васильева  $V_C^\lambda$  при  $\lambda \equiv 0$  через  $V_C^0$ . Пусть  $z, z' \in V_C^0$ . Рассмотрим две системы  $STS(V_C^\lambda, z) = STS(C, y)^0$  и  $STS(V_C^\lambda, z') = STS(C, y')^0$ , где  $z = (y + x, |x|, x)$ ,  $z' = (y' + x', |x'|, x')$ . Пусть  $\pi(STS(C, y)) = STS(C, y')$ . Тогда несложно видеть, что дубликатор  $\sigma_\pi$  подстановки  $\pi$  переводит  $STS(C, y)^0$  в  $STS(C, y')^0$ . Действительно,  $\sigma_\pi(\{i, n+1, i+n+1\}) = \{\pi(i), n+1, \pi(i)+n+1\}$ ,  $\sigma_\pi(\{i, j, k\}) = \pi(\{i, j, k\}) \in STS(C, y')$ ,  $\sigma_\pi(\{i+n+1, j+n+1, k\}) = \{\pi(i), \pi(j)+n+1, \pi(k)+n+1\} \in STS(C, y')^0$ .  $\square$

Компоненту  $R_j^n$  кода Хэмминга  $H^n$  длины  $n$  назовем *протыкающей* нули и единицы функции  $\lambda$ , если  $R_j^n$  содержит и нули и единицы функции  $\lambda$ .

Рассмотрим булеву функцию  $\lambda$ , определенную на коде Хэмминга  $H^n$  длины  $n$ . Рекуррентно определим функцию  $\lambda_N$  на коде  $H^N$ , положив  $\lambda_n \equiv \lambda$  и для  $y \in H^{(N-1)/2}$

$$\lambda_N((y, 0^{(N+1)/2})) + R_{(N+1)/2}^N = \lambda_{(N-1)/2}(y).$$

Пусть  $C$  – совершенный код длины  $N$ , полученный из кода  $V_{H^n}^\lambda$  длины  $2n+1$  посредством  $s$ -кратного применения конструкции Васильева с нулевой функцией,  $s = \log(N+1) - \log(2n+2)$  (далее для кода Васильева важно будет указывать, какой длины код Хэмминга и какая функция использовались для построения этого кода). Тогда верно следующее сведение

**Лемма 5.** 1. Код  $C$  длины  $N$  эквивалентен коду Васильева  $V_{H^{(N-1)/2}}^{\lambda_{(N-1)/2}}$ .

2. Если  $R_j^{(N-1)/2}$  протыкает нули и единицы функции  $\lambda_{(N-1)/2}$ , то  $R_j^N$  и  $R_{j+(N+1)/2}^N$  протыкают нули и единицы  $\lambda_N$ .

*Доказательство.* 1. Код  $C$  длины  $N$  имеет ранг на единицу больше, чем ранг кода Хэмминга той же длины. Известно, что всякий такой код эквивалентен коду Васильева  $V_H^{\lambda_{(N-1)/2}}$  для некоторой функции  $\lambda$  и некоторого кода Хэмминга  $H$  длины  $(N-1)/2$ . Однако для доказательства теоремы 4 нам важно убедиться, что исходный код Хэмминга длины  $n$  содержится как подкод в коде Хэмминга последней итерации при построении кода  $C$ . При  $s = 1$  имеем  $N = 4n + 3$  и подстановка

$$\varphi = \prod_{i=0}^n (n+i, 3n+2+i, 2n+2+i),$$

являющаяся произведением циклов длины 3, фиксирующая каждую из первых  $(n-1)/2$  координатных позиций, переводит код  $V_{H^n}^\lambda$  в код  $C$ . Для  $s > 1$  аналогичным образом, используя индукцию по  $s$ , можно выписать соответствующую подстановку.

2. Рассмотрим код Хэмминга  $H^{(N-1)/2}$ . Пусть  $j \leq (N-1)/2$ ,  $y \in R_j^{(N-1)/2}$ . Тогда так как  $(y, 0^{(N+1)/2}) \in R_j^N$ , то функция  $\lambda_N$  является  $R_j^N$ -протыкающей.

Пусть  $y = \sum_{m=1, \dots, r} \{i_m, j, k_m\} \in R_j^{(N-1)/2}$ . Тогда вектор  $y' = y + \sum_{m=1, \dots, r} \{k_m, (N+1)/2, k_m + (N+1)/2\} + \{j, (N+1)/2, j + (N+1)/2\}$  принадлежит компоненте  $y + R_{(N+1)/2}^N$ , следовательно  $\lambda_N(y') = \lambda_N(y)$ . С другой стороны,  $y' = \sum_{m=1, \dots, r} \{i_m, k_m + (N+1)/2, j + (N+1)/2\}$  принадлежит компоненте  $R_{j+(N+1)/2}^N$  и следовательно  $\lambda_N$  содержит и нули и единицы в компоненте  $R_{j+(N+1)/2}^N$ , так как обладает таким свойством в  $R_j^N$ .  $\square$

**Теорема 4.** Пусть  $\lambda$  – нелинейная функция, протыкающая компоненты, число нулей и единиц  $\lambda$  различны. Тогда  $Tr(V_{H^N}^{\lambda_N}) = Tr(V_{H^{(N-1)/2}}^{\lambda_{(N-1)/2}}) + R_{(N+1)/2}^N$ .

*Доказательство.* В силу определения, функция  $\lambda_N$  не является линейной, следовательно согласно Следствию 1 для выполнения  $y' \in Tr(V_{H^N}^{\lambda_N})$  необходимо и достаточно, чтобы нашлись подстановка  $\pi \in S_N$  и вектор  $u \in F^N$  для любого  $y \in H^N$  такие, что

$$\lambda_N(y' + \pi_{y'}(y)) = \lambda_N(y') + \lambda_N(y) + u \cdot y. \quad (4)$$

Рассмотрим линейное пространство  $L = R_{n+1}^{2n+1} + R_{2n+2}^{4n+3} + \dots + R_{(N+1)/2}^N$ . Заметим, что  $L$  также может быть представлено как следующая линейная оболочка компонент (равенство пространств легко показывается взаимным включением друг в друга с учетом определения  $i$ -компонент):

$$L = \langle R_{n+1}^N, R_{2n+2}^N, \dots, R_{(N+1)/2}^N \rangle. \quad (5)$$

Пространство  $U = \{y \in H^N : u \cdot y = 0\}$  либо совпадает с кодом Хэмминга  $H^N$ , либо является его гиперплоскостью, то есть подпространством на единицу меньшей размерности. Заметим, что всякая гиперплоскость кода Хэмминга  $H^N$  пересекается с любым линейным подкодом кода  $H^N$  либо по половине его векторов, либо является его надпространством.

Отсюда имеем следующие случаи:

1.  $|U \cap L| = |L|/2$ ;
2.  $L \subset \{y \in H^N : u \cdot y = 0\}$ .

Случай 1. Пусть  $|U \cap L| = |L|/2$ . Если  $y$  пробегает произвольный класс смежности  $a + L$  по подкоду  $L$  в равенстве (4) тогда, так как  $\lambda_N$  постоянна на  $L$  и, следовательно постоянна на любом классе смежности по подкоду  $L$ , левая часть равенства (4) принимает ровно половину нулей и единиц для класса смежности  $a + L$ . Таким образом, функция  $\lambda$  имеет одинаковое число нулей и единиц на коде  $C = V_{H^{(N-1)/2}}^{\lambda_{(N-1)/2}}$ . Противоречие.

Случай 2. Пусть  $L \subset U$ . Тогда любой класс смежности  $a + L$  является подмножеством  $U$  или не пересекается с ним. Рассмотрим равенство (4) при условии, что  $y$  пробегает класс смежности  $\pi_{y'}^{-1}(y') + R_i^N$ , где  $i$  кратно  $n + 1$ . В силу равенства (5) и условия  $L \subset U$ , имеем

$$\lambda_N(\pi_{y'}(R_i^N)) = \lambda_N(R_{\pi_{y'}(i)}^N) = \lambda_N(\pi_{y'}^{-1}(y')) + \lambda_N(y') + u \cdot \pi_{y'}^{-1}(y').$$

Другими словами,  $\lambda_N$  принимает постоянные значения на  $R_{\pi_{y'}(i)}^N$ .

Заметим, что в силу леммы 5, компонента  $R_j^N$  протыкает нули и единицы функции  $\lambda_N$  тогда и только тогда, когда  $j$  не кратно  $(n + 1)$ . Отсюда заключаем, что  $\pi_{y'}(\{1 \leq j \leq N : j \equiv 0 \pmod{n+1}\}) = (\{1 \leq j \leq N : j \equiv 0 \pmod{n+1}\})$ , так как в противном случае  $\lambda_N$  не будет постоянной на  $R_N^{\pi(i)}$ .

Итак, учитывая равенство (5), получаем  $\pi(L) = L$ . Поскольку код  $C$  разбивается на классы смежности по  $L$ , представителями которого являются кодовые слова  $H^n$ , то подстановка  $\pi$  переставляет эти классы смежности по  $L$ .

Рассмотрим представителей классов смежности по  $L$ , являющихся кодовыми словами веса 3 кода  $H^n$ . Заметим, что в классе смежности  $a + L$  существуют векторы веса 3 тогда и только тогда, когда вектор  $a$  имеет вес 3. Таким образом подстановка  $\pi_{y'}$  переставляет классы смежности  $\{i, j, k\} + L$ , где  $\{i, j, k\} \in H^n$ . Другими словами, найдется подстановка  $\sigma_{y'}$  из группы симметрий системы троек Штейнера кода  $H^n$  такая, что

$$\pi_{y'}(\{i, j, k\} + L) = \sigma_{y'}(\{i, j, k\}) + L.$$

Откуда в силу того, что группа симметрий кода Хэмминга совпадает с группой симметрий его системы троек Штейнера, заключаем, что  $\pi_{y'}(y + L) = \sigma_{y'}(y) + L$  для любого  $y \in H^n$ . Тогда выполняется последовательность равенств:  $\lambda_N(y' + \pi_{y'}(y + L)) = \lambda_N(y' + \sigma_{y'}(y) + L) = \lambda(y' + \sigma_{y'}(y))$ .

Отсюда, подставляя  $y$  и  $y'$  из  $H^n$  в равенство (4) и предполагая, что  $u = (u', u'')$ , где  $u' \in F^n, u'' \in F^{N-n}$ , получим

$$\lambda(y' + \sigma_{y'}(y)) = \lambda(y) + \lambda(y') + u' \cdot y,$$

что влечет  $y' \in Tr(V_{H^n}^\lambda)$  согласно Теореме 2. □

Из теоремы 4, лемм 3 и 4 получаем основной результат данной работы.

**Теорема 5.** *Для любого  $n \geq 15$  существуют двоичные совершенные гомогенные коды длины  $n$ , не являющиеся транзитивными.*



**Замечания.** Заметим, что для кодов Моллара имеет место теорема, аналогичная теореме 3 (см., например, определение кода Моллара в [5]). Коды Моллара являются обобщением кодов Васильева, теорема несложно доказывается с учетом строения системы троек Штейнера кода Моллара, которая подробно описана, например, в работе [11].

**Теорема 6.** Если  $C$  – произвольный гомогенный совершенный код длины  $t$ ,  $H$  – код Хэмминга длины  $r$ , то код Моллара  $M(C, H)$  длины  $tr + t + r$  при  $f \equiv 0$  является гомогенным.

Таким образом, гомогенные совершенные коды можно строить, используя конструкцию Моллара, хотя следует отметить, что технически осуществить это будет существенно сложнее изложенного выше.

## Список литературы

- [1] Östergård P.R.J., Pottonen O. The perfect binary one-error-correcting codes of length 15: Part I – Classification // *ArXiv*, <http://arxiv.org/src/0806.2513v3/anc/perfect15>, 2009.
- [2] Borges J., Mogilnykh I.Yu., Rifà J., Solov'eva F.I. Structural properties of binary propelinear codes // *Advances in Math. of Commun.* 2012. V. 6. N 3. P. 329–346.
- [3] Mogilnykh I.Yu., Solov'eva F.I. Existence of transitive nonpropelinear perfect codes // *Discrete Mathematics*. 2015. V. 338. P. 174–182. DOI: 10.1016/j.disc.2014.11.001.
- [4] Rifà J., Basart J.M., Huguët L. On completely regular propelinear codes // *Proc. 6th Int. Conference, AAECC-6. LNCS.* 357 (1989) 341–355.
- [5] Соловьева Ф.И. Обзор по совершенным кодам // *Математические вопросы кибернетики*. Вып. 18: Сборник статей/Под ред Н. А. Карповой.-М.: Физматлит, 2013. С. 5–34.
- [6] Соловьева Ф.И., Августинovich С.В., Хеден У. О структуре группы симметрий кодов Васильева // *Пробл. передачи информ.* 2005. Т. 41. Вып. 2. С. 42–49.
- [7] Васильев Ю.Л. О негрупповых плотно упакованных кодах // *Проблемы кибернетики*. М: Физматгиз, 1962. Вып. 8. С. 337–339.
- [8] Krotov D.S., Potapov V.N. Transitive 1-perfect codes from quadratic functions // *IEEE Trans. Inform. Theory*. 2014. V. 60. N 4. P. 2065–2068.
- [9] Assmus E.F., Jr.; Mattson H.F. On the number of inequivalent Steiner triple systems // *J. Combinatorial Theory*. 1966. V.1. P. 301–305.
- [10] Малюгин С.А. О классах эквивалентности совершенных двоичных кодов длины 15. Препринт № 138. – Новосибирск: Институт математики СО РАН, 2004. С. 34.
- [11] Mogilnykh I.Yu., Solov'eva F.I. On symmetry group of Mollard code // *Electronic Journal of Combin.*, 2014, submitted.

Могильных Иван Юрьевич, Соловьева Фаина Ивановна  
Институт математики им. С.Л.Соболева СО РАН,  
Новосибирский государственный университет  
{ivmog, sol}@math.nsc.ru